Data protection and the 'right to be forgotten' in practice: a UK perspective

Article (Accepted Version)

Author's accepted version, pre-copy edit. This article will appear in the International Journal of Legal Information in 2017.

Data protection and the 'right to be forgotten' in practice: a UK perspective

Judith Townend[1]

Abstract: *We are in an uncertain and complex period for data protection and privacy in Europe, and especially so in the UK, following the result of the 'Brexit' referendum on 23 June 2016. Information law, and data protection in particular, are of increasing concern for those in the business of knowledge sharing and information dissemination: media organisations, academic institutions and libraries. The notion of the 'right to be forgotten' is particularly troublesome, as lawyers, archivists, historians and philosophers grapple with the theoretical and practical implications. This paper discusses a selection of recent European and British policy and legal developments, and discuss how they are changing social practice and citizens' engagement with information rights.*

[1] Judith Townend is lecturer in media and information law and the University of Sussex and until recently – and at the time of giving this paper - the director of the Information Law and Policy Centre at the Institute of Advanced Legal Studies.

Author's accepted version, pre-copy edit. This article will appear in the International Journal of Legal Information in 2017.

In this contribution to the International Association of Law Libraries annual course 2016 in Oxford, I consider data protection and the so-called 'right to be forgotten', a notion that has been preoccupying those of us working in information law research in recent years. It offers a perspective from the UK and focuses on developments that are likely to be particularly relevant to legal publishing and research.

Context

This paper is rooted in a socio-legal understanding of data protection, with an emphasis on specific human interactions with media and information law and policy. Socio-legal study requires not only considering legal doctrine, but also broader interpretations and impact of statute and case law – this might even include *inaccurate* interpretations of law. While individuals may be wrong in their assertions about law, these assertions are not irrelevant. Perceptions of law, often based on accounts offered by the media, play a significant role in shaping social behaviour. In this way, we must look at what people think the law says, and how that affects legal decision making and behaviour.

In 2012-13, I conducted a series of interviews with media specialist solicitors and barristers in the UK,[2] who had direct and regular experience of advising media organisations and defending or bringing claims against them. I was interested in the ways in which these specialised practitioners perceived a 'chilling effect' of media law: what

[2] As part of doctoral research at the Centre for Law, Justice and Journalism at City University London.

were the ways in which law deterred their speech in undesirable ways, with a cost for freedom of expression?

My primary interest was defamation law, which, at the time, was on the brink of reform in England and Wales. But I was also interested in privacy law: how was the developing tort of 'misuse of private information' and data protection affecting the work these lawyers were involved in? With this in mind I often began interviews with a fairly open question, asking the lawyers about the nature of their workload and their main concerns on a day-to-day basis.

It was clear, that despite the relatively small number of defamation claims in the courts each year,[3] libel was still a major concern for these lawyers, and especially so for lawyers advising and acting for media organisations. The growth of claims of breach of privacy and misuse of private information were also a concern but when I pressed my interviewees for specific numbers or evidence, they tended to say that defamation was still the dominant concern.[4]

In fact, data protection was not really much of a talking point at all: my interviewees would remind me of the Section 32 of the Data Protection Act 1998 (DPA) which provides exemptions from *some* of the Act's provisions for journalistic, literary or artistic purposes.

---

[3] Townend, Judith. 2013. 'Closed Data: Defamation and Privacy Disputes in England and Wales'. *Journal of Media Law* 5 (1): 31–44. doi:10.5235/17577632.5.1.31.

[4] Townend, Judith. 2015. 'Defamation, Privacy & the "Chill": a Socio-Legal Study of the Relationship between Media Law and Journalistic Practice in England and Wales, 2009-13'. PhD thesis. City University London.

As the UK's leading legal textbook for journalists, *McNae's Essential Law for Journalists*, states: 'although data protection has been in force for nearly three decades, most journalists know little about it, probably because threats of prosecution against journalists have been rare'. But, as the book's authors also note, 'this is changing'.[5] In the few years since I conducted the original research, it is clear that data protection is becoming a much more pressing issue for media lawyers and media organisations. Anecdotal evidence indicates that data protection is beginning to loom much larger for media organisations, which have a growing awareness of the regulator's (the Information Commissioner) ability to impose civil monetary penalties and pursue criminal prosecutions, and to the possibility of civil claims of compensation brought by an individual claimant under the DPA. This is a trend that looks likely to continue; in their recent article tracing the adoption of data protection claims in media litigation, legal practitioners Jennifer Agate and Owen O'Rourke predict an 'upward curve' in such claims.[6]

It is likely that those working in universities and other public institutions are also increasingly mindful of data protection law and policies, despite the longstanding existence of such provisions. With hacking and data losses regularly reported in the mainstream news, and an increasing if not total reliance on electronic technology for data storage, organisations are – or should be! - alert to their responsibilities

5 Hanna, Mark, and Mike Dodd. 2016. *McNae's Essential Law for Journalists*. 23rd ed., 358
6 O'Rorke, Jennifer Agate and Owen. 2016. 'Data Protection in Media Litigation'. *Communications Law*, no. 21 (July): 46–48.

under the data protection framework, and the implications for them, if they do not comply with statutory requirements.

The data protection landscape

It is worth very briefly considering this landscape for UK organisations: currently the most relevant piece of domestic legislation is the Data Protection Act 1998, based on the EU 1995 Directive. Also relevant to mention are the data protection and privacy related Articles of the EU Charter on Fundamental Rights (Articles 7 and 8), and Article 8 of the European Convention on Human Rights. Under Article 8, a right to protection against the collection and use of personal data forms part of the right to respect for private and family life, home and correspondence. Finally, Council of Europe Convention 108 is the first legally binding international instrument dealing explicitly with data protection.

For a number of years, a new European data protection package – consisting of a Regulation on data protection (GDPR) and a Directive on the police and criminal justice sector – has been making its slow way through the EU Parliament and Council. The overall objective for the EU Regulation was to establish a single, pan-European law for data protection so that international companies could simply deal with one law, not 28 different laws. The GDPR was designed to 'enable people to better control their personal data' and aims to modernise and unify rules to allow businesses to participate in the Digital Single Market,

while the Data Protection Directive for the police and criminal justice sector aims to protect the data of victims, witnesses, and suspects of crimes and harmonise laws to facilitate cross-border cooperation of police or prosecutors.[7] Both were adopted in April 2016, with the Regulation applying to member states on 25 May 2018, and a deadline of 6 May 2018 for member states to transpose the Directive into national law.

Since I originally proposed this paper and drafted the abstract, there has of course been a dramatic development in the UK. On 23 June the UK voted to leave the EU by 52% to 48%, based on a 72.2% turnout of the British electorate. The new Prime Minister Theresa May has said that 'Brexit means Brexit'. But what does that mean? Certainly there is a lack of clarity on what the UK's relationship with European law will be, and to what extent the GDPR will be adopted in domestic legislation by the deadline of 25 May 2018. The UK data protection regulator, the Information Commissioner's Office, initially released a statement on 24 June which included this passage:

> *If the UK is not part of the EU, then upcoming EU reforms to data protection law would not directly apply to the UK. But if the UK wants to trade with the Single Market on equal terms we would have to prove 'adequacy' - in other words UK data protection*

[7] European Commission. 2015. 'European Commission Press Release: Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market'. Europa.eu. December 15. http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

> *standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018*.[8]

However, that bit of the statement has now been removed in an updated version, replacing it with a less specific commitment that:

> *Over the coming weeks we will be discussing with Government the implications of the referendum result and its impact on data protection reform in the UK*.[9]

On 4 July the then Minister for Data Protection, Baroness Neville-Rolfe (she has since been replaced by Matt Hancock MP) said:

> *One problem is that we do not know how closely the UK will be involved with the EU system in future. On one hand if the UK remains within the single market EU rules on data might continue to apply fully in the UK. On other scenarios we will need to replace all EU rules with national ones. Currently it seems unlikely we will know the answer to these questions before the withdrawal negotiations get under way*.[10]

---

[8] For a copy of the original statement see Baines, Jonathan. 2016. 'An Adequate Response to Brexit?' *Informationrightsandwrongs*. July 28. https://informationrightsandwrongs.com/2016/07/28/an-adequate-response-to-brexit/.

[9] ICO. 2016. 'Referendum Result Response'. July 1. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/07/referendum-result-response/.

[10] Neville-Rolfe, Lucy. 2016. 'The EU Data Protection Package: The UK Government's Perspective'. *Gov.uk*. July 4. https://www.gov.uk/government/speeches/the-eu-data-protection-package-the-uk-governments-perspective.

Meanwhile, the ICO has published its guidance on GDPR with an overview of the law.[11] It is still relevant in the UK, it says, 'most obviously' for those operating internationally. Steve Wood, interim deputy commissioner, also notes that GDPR has several new features – for example on breach notification and data portability, of relevance to information rights professionals.[12]

At this stage, it is not possible to predict the extent to which the GDPR will be incorporated, or whether the UK will continue to observe the jurisprudence of the European Court of Justice. If the UK has negotiated membership of the single market, it seems likely that provisions of the GDPR will feature in domestic legislation.

The other aspect that is worth mentioning is the UK's membership of the European Convention on Human Rights and the Council of Europe. Theresa May has, contrary to earlier statements made in April 2016 while she was Home Secretary, indicated during her leadership campaign that she would not pursue withdrawal from the EU.[13] That does not necessarily mean that the Human Rights Act 1998 is safe from repeal, however. A new British Bill of Rights, which has been discussed

11 ICO. 2016. 'Overview of the General Data Protection Regulation (GDPR)'. July 7. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.
12 Wood, Steve. 2016. 'GDPR Still Relevant for the UK'. *ICO Blog*. July 7. https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/.
13 'Theresa May Will NOT Try To Take UK Out Of European Convention on Human Rights'. 2016. *RightsInfo*. June 30. http://rightsinfo.org/breaking-theresa-may-will-not-try-leave-european-convention-human-rights/.

for some time, could still be a possibility.[14] However, if the UK remains a member of the ECHR it will need to abide by the judgments of the Court on privacy and data protection related rights, whether or not new human rights domestic legislation is introduced.

The overriding message is that this landscape is uncertain. This paper now turns to two specific aspects of data protection, which will remain relevant to UK society and publishing and research, Brexit or no Brexit, ECHR withdrawal or otherwise: the so-called 'right to be forgotten', and transfer of data from the European Union to the United States.

The right to be forgotten

The 'right to be forgotten' also known as the 'right to erasure' is an aspect of data protection that has garnered particular attention in the last few years. Both phrases are actually quite unhelpful: they suggest that it is possible to effectively erase information from memories as if there is a gadget for blitzing memories, like the neuralyzer device in the *Men in Black* film, or a medical procedure like the one seen in *Eternal Sunshine of the Spotless Mind*, which helps the character Joel, played by Jim Carey, forget his ex-girlfriend. The phrase indicates something a bit different from what the law is trying to achieve.

This notion is recognised in European law, in the 1995 Directive which gives a subject erasure rights under Article 12, and in the court's

[14] Elgot, Jessica. 2016. 'UK Bill of Rights Will Not Be Scrapped, Says Liz Truss'. The Guardian, August 22, sec. Law. https://www.theguardian.com/law/2016/aug/22/uk-bill-of-rights-will-not-be-scrapped-says-liz-truss.

application of the directive, most notably in the CJEU's decision in the *Google Spain v Costeja Gonzalez* case in 2014.[15] The 'right to be forgotten' phrase is also specifically included in Article 17 of the GDPR.

The *Costeja* case in Spain, which increased media interest and public awareness of this troubling and ambiguous notion, concerned name search links to a Spanish newspaper item about a real-estate auction for the recovery of social security debts in 1998. The preliminary ruling by the CJEU established not only that Google was a data controller, but that individuals have the right - under certain conditions - to request search engines to remove links with personal information about them. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing.[16]

At the same time, it was established that the 'right to be forgotten' is not absolute but needs to be balanced against other fundamental rights, such as freedom of expression.[17] Therefore a case-by-case assessment is needed considering factors such as the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information. The role the person plays in public life may also be relevant.

15 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. 2016, Case C-131/12. CJEU Grand Chamber.
16 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. 2016, Case C-131/12. CJEU Grand Chamber. para 93.
17 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. 2016, Case C-131/12. CJEU Grand Chamber. para 85.

Media coverage of this case and subsequent developments on the 'right to be forgotten' has been quite mixed: some was reasonably nuanced; some was quite dramatic with descriptions of censorship and Orwellian erasure.[18] The issue that many media commentators have with the 'right to be forgotten' is that it impacts on accurate record keeping, potentially influencing historical understanding of events. For the founder of Wikipedia, Jimmy Wales, it was 'one of the most wide-sweeping internet censorship rulings that [he had] ever seen'.[19]

In response to the ruling, Google implemented a system in which individuals could make requests to them to ask for material to be removed. These decisions can be appealed to the domestic data protection regulator – in the UK this would be the Information Commissioner's Office (ICO), which has offices in England, Wales, Scotland and Northern Ireland. This is part of work in progress that needs further regulatory attention.

This system has also included notifying webmasters, including media organisations, when their content was removed from name search results.[20] The effect was counter-productive for the complainant: some media organisations chose to re-publish stories that had been de-listed giving the information renewed publicity on their own sites and through

[18] See, for example: Hume, Mick. 2015. 'The EU Is Digging Orwell's "memory Holes" across the Internet'. *Spiked Online*. August 6. http://www.spiked-online.com/freespeechnow/fsn_article/the-eu-is-digging-orwells-memory-holes-across-the-internet#.V-04hjXdCUk.
[19] Lee, Dave. 2014. 'Google Ruling "Astonishing", Says Wikipedia Founder Wales'. *BBC News*, May 14, sec. Technology. http://www.bbc.co.uk/news/technology-27407017.
[20] See, for example, Lee, Dave. 2014. 'BBC to Publish "Right to Be Forgotten" Removals List'. *BBC News*, October 17, sec. Technology. http://www.bbc.co.uk/news/technology-29658085.

Google. It also led to mistakes about who had requested the item should be removed – one might expect it would be the main subject of a story but this is not necessarily the case – see for example, a story of a delisting reported by the BBC's Robert Peston.[21]

Another issue – which is relevant to the handling of any type of online restriction – is the extra jurisdictional treatment of content. Something may be removed from search results in the UK, but it can still appear in Google US results and so on. How do national courts deal with this conundrum? Is it enough to have localised geoblocking to enforce a 'right to be forgotten'? And how does one continue to enforce it? Could we simply end up in a game of perpetual Whack-a-Mole?

The implications for academic research are also worthy of attention. As researchers we often delve into archives and re-earth material that may never have been in digital form, or concerned events many years ago. If such material concerns personal information about living people and is given new prominence online, what are the considerations that need to be made? One possibility is to develop ethical principles for research – which may or may not be in friction with law – on the digital treatment of recent historical information that concerns living people.

The main ramification of the *Costeja* case seems to have been the introduction of new procedures for the delisting of search results, with

[21] Peston, Robert. 2014. 'Why Has Google Cast Me into Oblivion?' *BBC News*, July 2, sec. Business. http://www.bbc.co.uk/news/business-28130581.

limited impact on source material. However, in what may be the first case of its kind, a court in Belgium ordered the alteration of the material at source.[22] The Belgian Court of Cassation ordered the anonymisation of a historical news piece about a road traffic accident; it found that continued publication was a violation of the applicant's Article 8 rights under the ECHR. The applicant, a medical doctor, had been convicted of drink driving in 1994. At this point, it is difficult to envisage a similar outcome in the UK, and one can imagine the outrage with which the national press would greet such a finding. But, as Hugh Tomlinson notes in his report of the case, the English courts are yet to engage with the issue.[23]

Clearly, if such a finding was made domestically or at the European level, it could have huge significance for the handling of archives containing material on criminal and civil law, and especially for data relating to convictions. Particularly so in the UK context where we usually report the full names of individuals involved in criminal cases; usually we would expect this information to be provided – and not just the names of those on trial, but also victims, witnesses and other relevant parties.

If other courts follow the Belgian court's lead in removing archive material, where does one stop? Would it rationally follow that there

[22] *Olivier G v Le Soir*, 29 April 2016, C.15.0052.F.
[23] Tomlinson, Hugh. 2016. 'Case Law, Belgium: Olivier G v Le Soir. "Right to Be Forgotten" Requires Anonymisation of Online Newspaper Archive'. *Inforrm's Blog*. July 19. https://inforrm.wordpress.com/2016/07/19/case-law-belgium-olivier-g-v-le-soir-right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive-hugh-tomlinson-qc/.

should be a positive requirement on organisations to actively monitor their online archives for outdated material? And what about Internet archives and library archives, not available on the open web, do they also have to be altered? The 'right to be forgotten' remains a problematic concept, both from a legal and ethical perspective.

EU-US data transfer

The second and final aspect of data protection this paper briefly highlights is the transfer of data from Europe to the US.

According to research published by the European Commission in July 2015, Europeans 'overwhelmingly believe they should always have the same rights and protections over their personal information regardless of the country in which the public authority or private company offering the service is established'.[24] This an issue that has preoccupied one very enterprising Austrian law student, Maximilian Schrems. After becoming frustrated with the lack of control he could exercise over the data that Facebook held on him and the basis by which Facebook Ireland was transferring data to its US servers, he began a series of legal challenges that are described on his website as 'EU v Facebook'[25] – with a mission to investigate whether EU Data Protection laws are enforceable in practice. In actuality, the implications are far wider reaching than Facebook. Schrems originally complained to the Irish Data Protection

[24] European Commission. 2015. 'Special Eurobarometer 431: Data Protection'. http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.
[25] http://europe-v-facebook.org/EN/en.html.

Commissioner, then to the Irish High Court, which referred the question to the European Court of Justice.

The CJEU ruled in October 2015 that the Irish Data Protection Commissioner was permitted to consider the question of its adequacy of the Safe Harbor regime, despite a Commission decision that recognized its validity. Crucially, although it did not decide the case itself, the CJEU found that the 'Safe Harbor' agreement which permitted transfer of data between the US and Europe was invalid and did not provide adequate protection, particularly with regard to safeguards against mass surveillance.[26]

It was thus for the Irish Data Protection Commissioner to decide whether, pursuant to the Data Protection Directive, transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data.

Needless to say, that outcome would be hugely significant, both legally and practically speaking. The latest development to report is that the US Government is seeking to join the Irish case as a party. The Schrems campaign suggests that the US government likely wants to defend its surveillance laws before the European Court.[27]

[26] Maximillian Schrems v Data Protection Commissioner. 2015, Case C-362/14. CJEU (Grand Chamber).
[27] Europe-v-Facebook.org. 2016. 'NSA Mass Surveillance: US Government Wants to Intervene in European Facebook Case'. http://www.europe-v-facebook.org/PR_MC-US.pdf.

More generally, the CJEU's decision in *Schrems* has led the European Commission to introduce a new Privacy Shield, which was adopted on 12 July, to replace the previous Safe Harbor agreement. The Article 29 Working Party, which was critical of the draft Privacy Shield decision, welcomed improvements but remained concerned on both the commercial aspects and the access by US public authorities to data transferred from the EU.[28]

Conclusion: Access to legal material

This paper only touches the surface of data protection developments affecting the UK, let alone the many countries represented by the members of the International Association of Law Libraries at the annual conference. To summarise, it is a narrative of uncertainty, with regard to the development of the EU GDPR in domestic law, transfer of data between the US and Europe, and the further evolution of the so-called 'right to be forgotten'. A question for further discussion within the IALL might be: what does all this mean for archivists and librarians? In anticipation of this debate, I offer these concluding thoughts:

First, regardless of the UK's changing relationship with European law, there are likely to be more 'right to be forgotten' cases centering on source material from media and research sites, as well as search engines and social media platforms, and this presents the UK and other

[28] Article 29 Working Party. 2016. 'Article 29 Working Party Statement on the Decision of the European Ommission on the EU-U.S. Privacy Shield'. European Commission. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

countries with difficult philosophical as well as practical questions about how states should balance digital privacy rights with the very important public function of preserving accurate and full records.

Second, the possible use of data protection in areas where defamation previously dominated is significant. It provides a tool for claimants to request removals of out of date or inaccurate material, a different test than that demanded in defamation – where the claimant would have to show that the material was defamatory of them, not merely inaccurate or out of date.

Third, legal records are going to present a particular problem: many 'right to be forgotten' cases and incidents to date have concerned criminal records data, and the UK tradition for naming the subjects of court cases in media and law reports, presents an interesting conundrum. Here, the friction is between freedom of expression and open justice, on the one hand, and rights to privacy and rehabilitation on the other. The views and experience of law librarians and legal information specialists will provide an invaluable contribution to the shaping of policy in this area.